Contents lists available at GrowingScience

Management Science Letters

homepage: www.GrowingScience.com/msl

Multi-banking ATM system services using biometrics

Harsha Patil[a*], Vikas Mahandule[a], Lekharaj Khachane[a] and Shruti Narkhede[a]

[a]*MIT Arts Commerce and Science College Alandi Pune, India*

CHRONICLE

Article history:
Received: December 21, 2023
Received in revised format:
January 25 2024
Accepted: March 3, 2024
Available online:
March 3 2024

Keywords:
ATM
OTP
Face Recognition

ABSTRACT

Automated Teller Machine (ATM) transactions are now regarded as secure, dependable, and unavoidable for meeting our financial obligations. The conventional method of utilizing an ATM requires the use of a debit card. But occasionally users run out of money in their accounts or forget their cards, which makes it difficult to execute a purchase. Mobile phone use has been an unavoidable development, similar to ATM usage. By connecting these electronic devices, it has become possible to make cash withdrawals that are both quick and secure without the use of a debit card, or "card-less cash withdrawals". For user authentication, face detection, OTP and fingerprint scanning are used. Three tiers of security are constructed by this. If all three parameters are authenticated then and then only the user is allowed to the banking transaction.

1. Introduction

Automatic Teller Machine or ATM, is a common acronym. To use ATMs to obtain cash at any time and anywhere. PINs(Personal Identification Number) can be used to complete transactions on conventional ATM machines. Biometric verification is necessary for secure transactions. The field of facial recognition is young and contentious. The biometric industry standards are currently being tested, and biometric legislation and regulations are in the works. The three most well-known attacks on ATMs are skimming, PIN logging, and integrity violations. Other attacks against mobile devices include the installation of fake portable programs, key recording software, and the theft of PIN numbers while being transmitted. In addition, this attack may be a combination of the two types of attacks mentioned earlier. It is known that attackers try to obtain user data stored on the magnetic strip on the back of ATM cards. The main character that can be used to verify ownership of an ATM card is the PIN. It suggests that as long as the secret PIN entered is correct, anyone can use an ATM to view bank records. As a result, they can take money from that account effectively without having to worry about user authentication when the ATM card and passwords are lost or stolen. So it's clear that user authentication is the most challenging issue that has emerged in ATM card security (Narteh, 2013).

2. Literature Survey

Automated Teller Machine, or ATM, is a common acronym. By using ATMs, we can obtain cash at any time and anywhere. Performing secure transactions requires the use of biometric authentication with biometrics is a contentious and evolving field. Currently, biometric laws and norms and guidelines are being developed for the biometric sector and are tested. There were three well-known attacks against ATM: PIN logging, skimming, and integrity violations. Additionally, there are assaults on cell phones: phony versatility setting up applications, programming key, logging, and PIN number theft during transfer.

* Corresponding author.

E-mail address: hrpatel888@gmail.com (H. Patil)

doi: 10.5267/j.msl.2024.3.002

Besides that, an attack could also be a combination of the aforementioned two type's attacks (Nuthan et al., 2015). The information may also be misused through a side channel attack. It is found that attackers try to approach users. Information stored on a magnetic strip that is present at the cards back for an ATM. The major characters are secret PINs. It can be used to verify who the ATM card belongs to (Vishwakarma et al., 2020). It suggests that anyone could access the financial records. The secret PIN entered into the ATM machine is correct. So, the loss or theft of the ATM card and passwords can effectively remove money from the account without the problem of user authentication (Jimoh & Babatunde, 2014; Jegede, 2014).

This project offers a solution to these problems. There are three levels of security while using an ATM. It introduces facial recognition and biometric verification measures in conjunction with the generation of OTP process. The user's fingerprint and facial pictures are required to be checked and verified while logging in. A user will receive an OTP that verifies their authenticity. After confirming each of the three variables, the user will have access to the ATM operations as permitted (Selina & Oruh, 2012; Agrawal et al., 2021). It always leaves very little room for scams. Using OTP ensures that the session will be fresh. So, this project's objectives are to increase ATM exchange security (Gupta, 2022).

3. System Architecture

In addition to facial recognition and fingerprint sensors, we have integrated OTP verification into our ATM systems. Upon initiating a transaction, you will receive a One-Time Password on your registered mobile device. This OTP serves as a temporary access code that complements the biometric authentication process, ensuring an extra level of security. Once the OTP is entered correctly, the transaction can proceed, guaranteeing that only authorized individuals can perform banking operations.

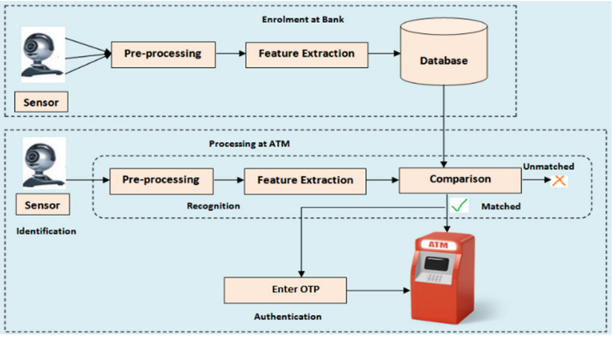


Fig. 1. System architecture.

The facial recognition sensor, which is typically a camera, captures the user's facial image. It analyses various facial features such as eye distance, face shape, and unique facial landmarks to create a unique biometric template for each individual. To verify the user's identity, this sensor employs advanced algorithms that compare the captured image with the stored facial data and also using the landmarks it checks for the liveliness in the video.

Then the fingerprint sensor scans the unique patterns on a user's fingertip. It analyses the ridges, furrows, and minutiae points of the fingerprint using either optical or capacitive technology. To authenticate the user, this sensor converts the captured fingerprint into a digital template, which is then compared to the stored fingerprint data.

Simple Mail Transfer Protocol (SMTP) is used to send codes via email. It involves setting up an SMTP server or using a third-party service, generating unique OTP codes, composing an email with the OTP, establishing an SMTP connection, sending the email, and verifying the OTP code provided by the user. This method provides a secure and convenient way for users to receive and use OTPs for authentication purposes. If everything matches with the user data then the user will be able to go to the banking services otherwise the transaction gets eliminated.

4. Methodology

The basic working of our system is in three parts where the first phase is regarding the registration of the user, the user has to register at the bank where his biometrics details will be taken and stored in our database. The next step is at the ATM machine where the user tries to access the banking system by signing in into the machine by authenticating his credentials. The third step is banking, where the user gets access to his account where he can see his balance or withdraw the amount of money from various bank accounts.

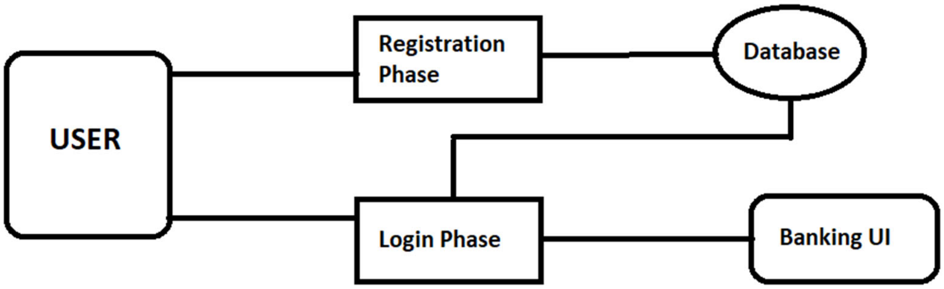


Fig. 2. Different Phases of our system

4.1 Registration Phase

1) In the registration process the customer has to enter his Username and E-mail id through which he wants to receive the OTP.
2) The user's facial image is captured and stored in the database which uses the 68-Landmark module to extract unique features from the face and store it in the database.
3) To capture the fingerprint of the user the R307 device is used. A capture method provided by the pyfingerprint in-built library is used to register the user's fingerprint to the database.
4) The user's personal details are acquired and stored in the database.

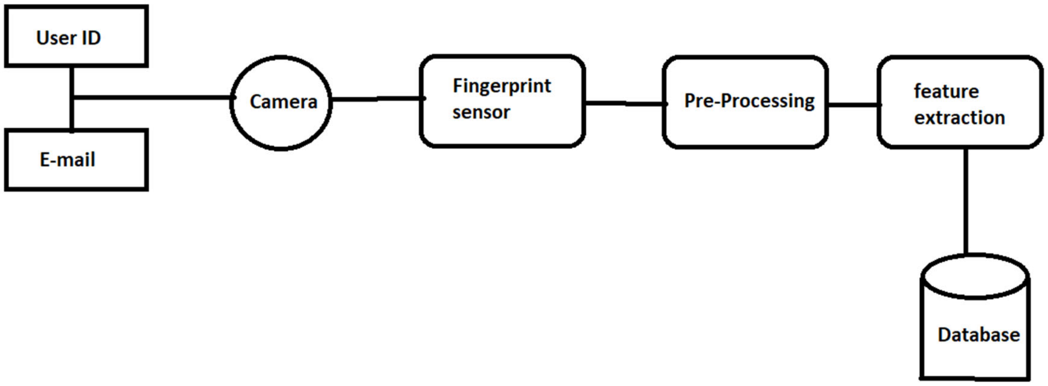


Fig. 3. Registration process.

4.2 Login Phase

1) The camera is always on and captures the image of the person in front of the camera. The captured image is checked whether it is a live image. It is verified through blinking of eyes using ratio analysis. After successful Verification of liveness it verifies the face of the person. After successful verification a Fingerprint Authentication is to be done.
2) The fingerprint of the person is read by the R307 and then verified. Upon verification a success message is shown on the screen. An OTP is generated on completion of the fingerprint authentication process.
3) A 4-digit randomly generated OTP will be sent to the user's E-mail id which was given at the time of registration process. Upon successful verification of the OTP the user can do banking transactions.
4) If any of the parameters doesn't match then the transaction will fail.

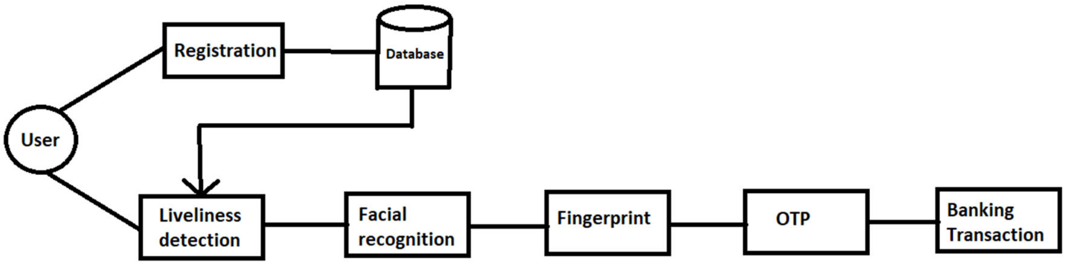


Fig. 4. Login phase

4.2.1 Face Detection algorithm

To Recognize and locate a person's face within an image or video frame.

Facial Landmark Localization: Determine key facial landmarks such as the corners of the eyes, nose, and mouth.
Feature Encoding: Using CNN, analyze the geometric relationships and measurements between facial landmarks to create a unique representation of the face.
Pre-Processing: Preprocessing in facial recognition refers to the steps taken prior to feature extraction to improve data quality and standardization. It includes the following:
Image Quality Evaluation: Assess the quality of captured facial images by taking into account factors such as blurriness, illumination, and noise level.
Normalization: Normalization is the process of standardizing facial images to eliminate variations in scale, rotation, and translation, resulting in consistent and comparable features.
Noise Reduction: Filters or statistical algorithms can be used to reduce unwanted variations caused by sensor imperfections, environmental factors, or image artefacts.

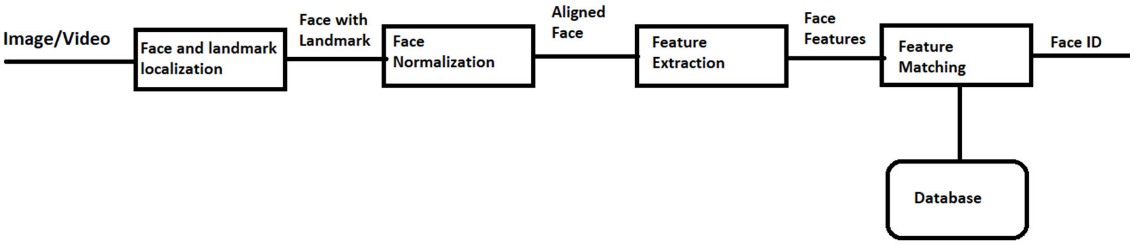


Fig. 5. Face Recognition Algorithm

4.2.2 Fingerprint-Detection Algorithm:

Data capture: Biometric data such as fingerprints is captured using sensors or special graphic devices designed for different models.
Pre-Processing: Captured biometric information goes through pre-processing procedures to improve its quality and standardize its type. This may include noise reduction, image enhancement, normalization or filtering to remove artifacts and distortions.Feature Extraction: Feature extraction algorithms first analyze biometric data to identify and extract unique features. These algorithms focus on capturing the most distinctive biometric patterns, such as fingerprint patterns, facial features or iris beauty.
Feature representation: Extracted features are represented in a compact and efficient way. This representation may use mathematical models, image vectors, or other numerical descriptors that capture the unique features of the biometric modality.
Template Creation: Creating a template based on the extraction and representation process as a reference for further processing or validation. This model contains important information needed to compare and validate biometric data.
Pairing and Comparison: Comparison of extracted features from biometric devices with stored samples during inspection or verification.
Matching algorithms use mathematical or statistical methods to calculate similarities or differences between two sets of features.
Decision Making: The decision to accept or reject a biometric sample based on similarity scores or thresholds. If the similarity crosses the threshold, the person is identified or identified.
Fingerprint accuracy can vary depending on many factors, such as the quality of the sensor, the algorithm used for fingerprint recognition, and the use of the sensor in different products. In general, modern fingerprint sensors have achieved a high level of accuracy.

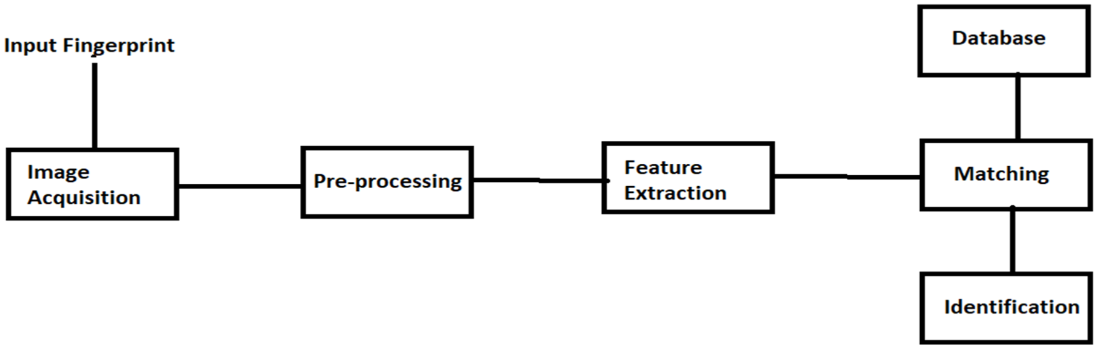


Fig. 6. Fingerprint detection algorithm

4.3 Banking Phase

1) After successful login UI interface can be seen. In which we can see Banking Services like cash withdraw and balance check. User can access multiple bank accounts for the cash withdrawal and balance enquiry.
2) For withdrawal the user the has to enter the amount of money he has to withdraw from the respective bank account after verifying the amount the money will be withdrawn. And the updated bank balance can be seen.

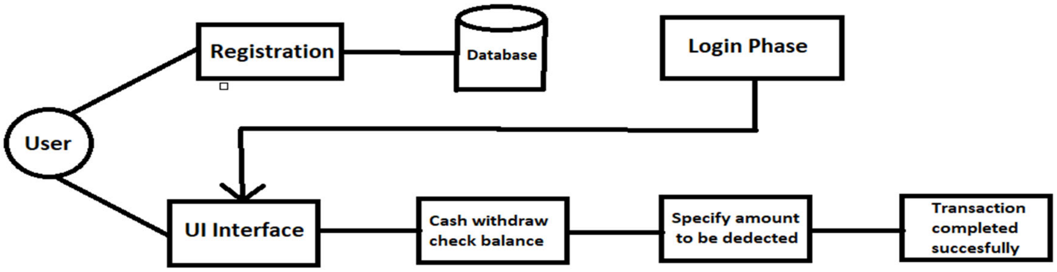

Registration
Database
Login Phase
User
UI Interface
Cash withdraw check balance
Specify amount to be dedected
Transaction completed succesfully

Fig. 7. Banking Phase.

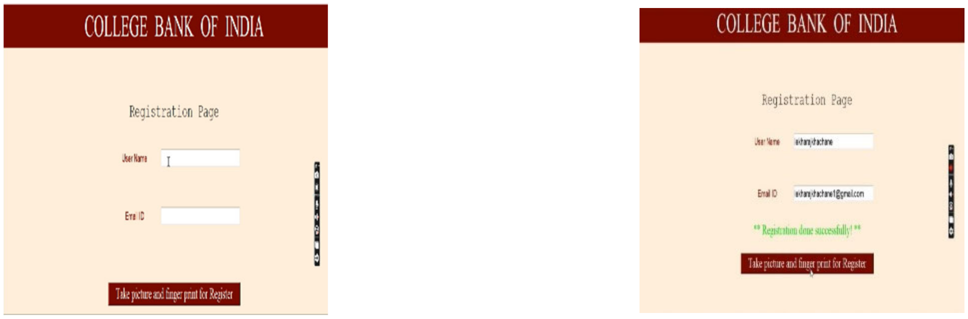
Python Libraries used:

A Python library is a collection of pre-written code that extends the functionality of the Python programming language. It has models, functions, and classes designed to perform specific tasks, making it easy for developers to perform complex tasks without reinventing the wheel. Python libraries cover many areas, including data analysis, machine learning, web development, graphics, networking, and more. Developers can use existing code to save time, increase efficiency, and add advanced functionality to their project applications by deploying and using these libraries in their projects.

```
pip install numpy
python -m pip install --upgrade pip
pip install pandas
pip install opencv-python
pip install pillowpip install face-recognition
pip install mysql-connector-python
pip install requests
pip install tensorflow
pip install keras
pip install pyfingerprint
```

5. Results and discussion

In order to register, the user must input his email address and username in the form where he has to enter his details like Username, email address, and then he has to register his face and fingerprint after that all the data will be stored in database.



COLLEGE BANK OF INDIA

Registration Page

User Name

Email ID

Take picture and finger print for Register

Fig. 8.1

COLLEGE BANK OF INDIA

Registration Page

User Name: vikhanjitachane

Email ID: vikhanjitachane1@gmail.com

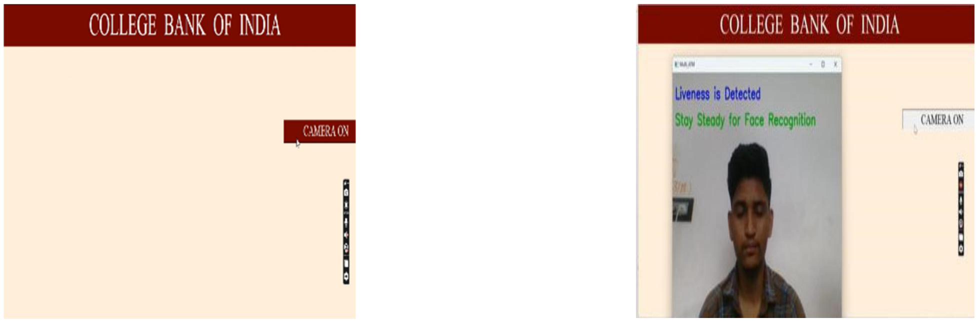
** Registration done successfully! **

Take picture and finger print for Register

Fig. 8.2

Fig. 8. User registration at bank.

The user must select the “camera on” button to begin a bank transaction.
liveliness will be detected by the camera as the user will blink his eyes, after that facial recognition process will start and if it verifies then it will then move on to the finger print recognition step.

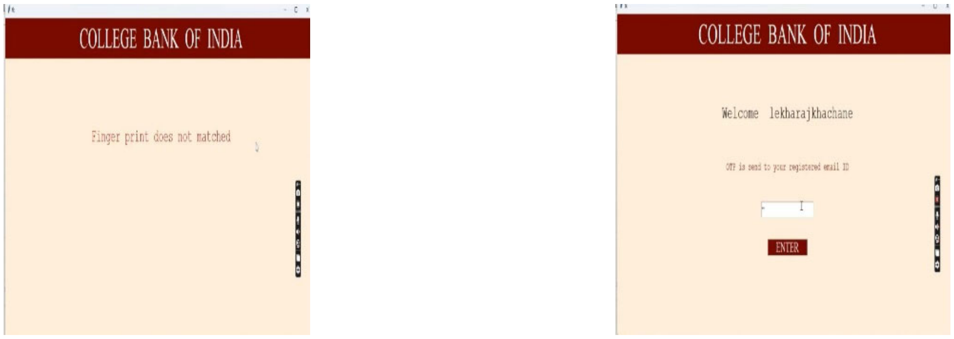


Liveness is Detected
Stay Steady for Face Recognition

Fig. 9.1. **Fig. 9.2.**

Fig. 9. Liveliness detection & face recognition

The phrase “fingerprint does not match” will appear if an unauthorized user attempts to validate their fingerprint. If the fingerprint matches, the user will generate an OTP that must be entered.



Finger print does not matched

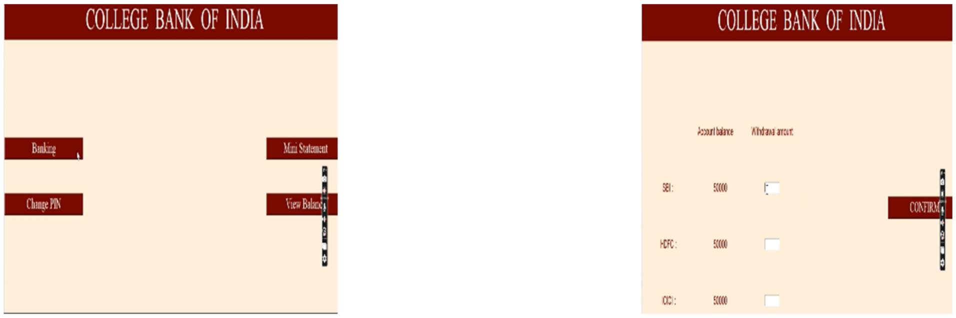
Welcome lekharajkhachane

OTP is send to your registered email ID

Fig. 10.1 **Fig. 10.2**

Fig. 10. OTP Verification

After the OTP matches, the user can continue with the bank transaction and begin carrying out the transactions.

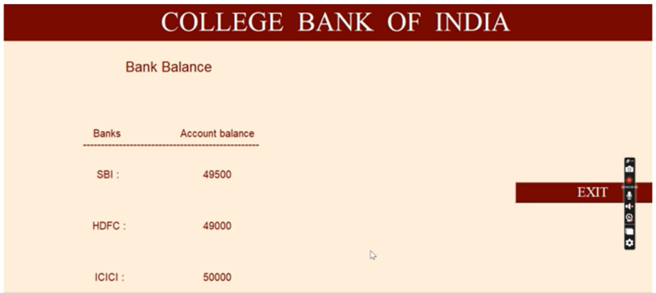


	Account balance	Withdraw amount
SBI :	50000	
HDFC :	50000	
ICICI :	50000	

Fig. 11.1 **Fig. 11.2**

Fig. 11. Bank transaction process.

After the transaction, the updated balance can be seen on the screen for multiple banks, and data in the bank database will also be updated.



Bank Balance

Banks	Account balance
SBI :	49500
HDFC :	49000
ICICI :	50000

Fig. 12. Successful completion of transaction.

The false recognition rate (FAR) and false rejection rate (FRR) of commonly available fingerprint scanners for smartphones and other devices are typically between 0.1% and 1%. This means that it is less likely to reject an unauthorized fingerprint (FAR) or a valid fingerprint (FRR).In other words, if the FAR value of a fingerprint is 0.10%, this means that for every 1,000 fingerprints, approximately 10 fingerprint that does not match the registered fingerprint will be accepted. Similarly, an FRR of 0.25% means that for every 1000 valid observations, approximately 25 fingers will be rejected.

The accuracy of facial recognition using a 68-landmark module can be high, potentially reaching over 99% in well-implemented systems with good quality images. However, accuracy can be affected by factors like lighting, pose, and occlusions. As compared to the existing method which involves carrying ATM card remembering passwords and also for different banks we have to carry different cards which is quite a hassle. Also the chances of cards being stolen or getting lost in this method. The use of facial recognition and fingerprint recognition in many ATMs provides security, simplifies the user experience, improves business efficiency, reduces fraud, increases reliability and scalability. This biometric technology helps create a safe and convenient banking environment that benefits both banks and their customers.

6. Conclusion

ATM’s are so efficient and practical for bank customers, the ATM's adoption as an electronic banking channel has had a favorable effect on the banking industry globally. However, the emergence of ATM fraud has been a threat for many banks around the world, and many banks are now working to eliminate the costs associated with theft.

The suggested approach may offer an efficient and realistic answer to the needs of the banking regulatory authority. Because it makes use of the elements of the current system, the technology used in the proposed system is also less expensive. To meet the needs of a customer base that prioritizes cash transactions, the model can also offer high withdrawal thresholds. Overall, it will have a positive impact on the banking industry and society by reducing the increase in crime related to ATM transactions.

References

Agrawal, S. S., Oza, P., Biswas, M., & Choksi, N. (2021). Enhanced Secure ATM authentication using NFC Technology and Iris Verification. *Scalable Computing: Practice and Experience*, *22*(2), 273-282.

Gupta, R. (2022). A Study on Growth and Usage of ATM/POS in India: Pre and Post Covid19. *Journal of Positive School Psychology*, 11872-11881.

Jegede, C. A. (2014). Effects of automated teller machine on the performance of Nigerian banks. *American Journal of applied mathematics and statistics*, *2*(1), 40-46.

Jimoh, R. G., & Babatunde, A. N. (2014). Enhanced automated teller machine using shortmessage service authentication verification. *African Journal of Computing & ICT*, *7*(1), 115-120.

Narteh, B. (2013). Service quality in automated teller machines: an empirical investigation. *Managing Service Quality: An International Journal*, *23*(1), 62-89.

Nuthan, K., Nagarathna, B. M., & Sumana Nayaka, R. L. (2015). An Automated Teller Machine*. International Journal of Novel Research in Computer Science and Software Engineering, 2*(1), 43-45.

Selina, O., & Oruh, J. (2012). Enhanced atm security system using biometrics. *International Journal of Computer Science Issues*, *9*(5), 352-357.

Vishwakarma, V., James, H., Bururu, R.K., & Matto, J. (2020). ATM Cash Replenishment with Clustering Series. *International Journal of Scientific & Engineering Research, 11*(5).